REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No.2 (2024)
http://www.veterinaria.org
Article received- Revised- Accepted-

Digital Proofs And Legal Admissibility: Understanding Electronic Evidence Under The Bharatiya Sakshya Adhiniyam

Dr. Anju Sinha[1*]

[1*]Assistant Professor (Selection Grade) Faculty of Law, University of Delhi.

ABSTRACT
The 'Bharatiya Sakshya Adhiniyam 2023' has repealed the 'Indian Evidence Act, 1872' and introduced significant provisions for the 'admissibility', 'relevance,' and 'reliability' of 'electronic evidence' in legal proceedings. This paper explores the legal framework under the 'Indian Evidence Act' and Bhartiya Sakshya Adhiniyam governing 'electronic evidence', focusing on its admissibility under Sections 61 to 65B. New methods are required to ensure the authenticity and integrity of evidence due to the transition from traditional physical evidence to electronic formats like emails, digital documents, and social media information. The Act tackles issues like the chain of custody, certification's function in digital evidence, and striking a balance between individuals' right to privacy and the process of legal discovery. Special emphasis is placed on the procedural requirements for presenting electronic records, with detailed analysis of court rulings on their applicability. Additionally, this paper reviews the challenges courts face in interpreting electronic evidence and suggests best practices for legal professionals in handling digital evidence under the new legislative regime.

Keywords: Electronic evidence, digital, data, document, technology

INTRODUCTION

Transmitting ideas from the physical to the digital realm facilitates social contact. The utilization of information and communication technology, including computers, smartphones, printers, digital cameras, and other gadgets, is central to the virtual world. In contrast to the physical world, there are numerous chances in the virtual world for crimes like 'hacking,' 'child pornography,' 'phishing,' and 'identity theft' to be committed. 'Electronic data' plays a significant role in establishing or refuting a truth or facts in dispute; data is used as evidence in court. Evidence, as defined by Black's Law Dictionary (2014), is anything that tends to prove or disprove an asserted fact. Evidence produced by 'mechanical' or 'electronic processes' is called "electronic evidence". 'Emails', 'text documents', 'spreadsheets', 'photos', 'graphics', 'database files', 'erased files', 'data backups', and 'files on floppy disks', 'zip disks', 'hard drives', 'tape drives', 'CD-ROMs', 'mobile phones', 'microfilms', 'pen drives', 'faxes', and other storage devices are all included, though not limited to. Until recently, there were no explicit provisions in the 'Indian Evidence Act,' of 1872 that acknowledged the admissibility and value of 'digital evidence.' It was not up to date with the advancements in current technology. Therefore, new legislation was needed to recognize transactions made via 'electronic data' interchange and other 'electronic communication' channels. As a result, the 'Information Technology Act' 2000 was passed.
The 'UNCITRAL' Model Law on Electronic Commerce serves as the foundation for the IT Act.(UN Model law,1996), The 'Indian Penal Code' 1860, the 'Banker's Book Evidence Act,' 1891, and the 'Indian Evidence Act of 1872', among other laws, are amended by the IT Act, which primarily recognizes transactions conducted through 'electronic data interchange' (i.e., communication between computers) and other forms of communication.Computer evidence, digital audio, digital video, mobile phones, and digital fax machines are all examples of 'electronic forms of evidence.' The Explanation to Section 79A of the IT Act also includes any information or evidence value that is kept or communicated electronically. During a civil or criminal case, courts may allow the use of 'digital evidence', including 'emails', 'digital photos', 'word processing documents', 'instant messaging histories', 'spreadsheets', 'internet browser histories', 'databases', 'contents of computer memory', 'computer backups', 'secured electronic records' and 'secured electronic signatures', 'GPS tracks', 'hotel electronic door logs,' 'digital video or audio', etc.

Section 2(t) of the IT Act defines the term 'electronic record' as – "data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche". The IT Act's Section 6 states that the government and its agencies may use electronic signatures and records. As a result, they are admissible in court. Therefore, admissible evidence must be shown to determine the merits of a case involving online contracts or e-crimes that need to be decided by a court.

Section 3 of the Evidence Act defines the term 'evidence', which reads as – "Evidence" means and includes—(1) all statements which the Court permits or requires to be made before it by witnesses about matters of fact under inquiry; such statements are called oral evidence; (2) all documents including electronic records produced for the inspection of the Court; such documents are called documentary evidence. Section 22A of the Evidence Act deals with when it is relevant to make an oral admission regarding the contents of electronic records.
Section 45A of the Evidence Act deals with the Opinion of the Examiner of 'Electronic Evidence.' Section 59 deals with Proof of facts by oral evidence. Section 67Adeals with proof as to digital signature. Section 73A deals with proof as to verification of the digital signature. Section 4 of the IT Act speaks about the legal recognition of electronic records. A

judge can determine whether evidence is admissible under Section 136 of the Evidence Act. The judge has the authority to inquire as to how the evidence presented is relevant to keep the proof focused on relevant facts and prevent it from straying from the boundaries of the case at hand. The judge must then determine the admissibility. The Supreme Court noted in State of Bihar v. Sri Radha Krishna(1983) that a document's admissibility is one thing, but its probative value is quite another, and the two cannot be mixed.

PROOF OF DOCUMENT AND ELECTRONIC EVIDENCE

At this juncture, let us now examine the pertinent provisions in the 'Indian Evidence Act ,1872' that address the proof of a document's contents. The pertinent sections of the Act that address proof of document contents are now available for review. In leading documentary evidence, producing and substantiating the original document is customary. The aforementioned norm is expressed in Section 61, which states that primary or secondary evidence may be used to prove the contents of documents. The document produced for the Court's examination is considered the 'primary evidence' as section 62 and section 63 list several kinds of 'secondary evidence.' The circumstances under which 'secondary evidence' may be offered are specified in section 65, which provides that if the 'original document is lost, destroyed, or in possession of an opposite party or public document or when the original document is not readily moveable, secondary evidence of its contents may be produced.'

Computerized assistance and operating systems in business cannot be brought before a judge. These computers use magnetic tapes (hard discs) to store their data. The electronic record that is generated from it needs to be printed out. Subsection (1) of section 65B allows the printout of an electronic record stored on magnetic media to be admitted into evidence without additional proof, provided that the requirements outlined in Subsection (2) are met.

Thus, compliance with sub-sections (1) and (2) of section 65B is needed to prove and make electronic records admissible. This inference is evident even from the wording of sub-section (4) of section 65B which permits the use of a certificate issued by the person specified in subsection (4) and certifying the contents in the way specified in the sub-section as evidence of the conditions stated in subsection (2). When it is certified by the individual listed therein that a computer printout's contents were produced by a machine satisfying sub-section (1)'s requirements, the sub-section admits 'electronic records.' As a result, subsection (4) offers an additional way to demonstrate an 'electronic record.'

Due to the greater vulnerability of 'electronic records' to manipulation, change, transposition, omission, etc., a trial that relies solely on using 'electronic data' as proof may become a mockery of justice without appropriate protections. Thereby it needs to satisfy three things, namely – 'Integrity of the data,' 'Integrity of the hardware/software,' and 'Security of the system.'

There, let us have a look at what happens when a party challenges the credibility of the evidence itself.

- If someone contests the veracity of an electronic record or piece of evidence based on allegations of system abuse, malfunctions, or interpolation, they must provide proof of the same beyond a reasonable doubt.
- Email evidence must be provided under Section 65B of the Indian Evidence Act, which mandates that a certificate be provided by a person holding a responsible position in computer administration. This is because email is a computer output of an electronic record.
- According to IT Act section 2(t), a "mobile" is a computer, and an SMS sent using a mobile device is an electronic record. Therefore, it must be proven under section 65B of the Indian Evidence Act, which calls for a certificate from a person responsible for the administration of the pertinent activities or the operation of that device.
- The party seeking to establish a C.D. must demonstrate whether the contested C.D. was created using a combination of the computer operating inside, other computers working sequentially throughout that time, or a different combination of computers.

In 'Anvar P.V v. P.K. Basheer'(2014), a three-judge bench of the SC ruled that "the computer output is unacceptable without conformity with Section 65B." It overruled the judgment of the two-judge SC Bench in 'State (NCT of Delhi) v. Navjot Sandhu alias Afzal Guru'(2005).

In the case of 'Tomaso Bruno v. State of UP'(2015), a three-judge bench of the apex court addressed the admissibility of evidence in a criminal proceeding. The Court held "that computer-generated electronic recordings are admissible in evidence at a trial provided they are proven under Section 65B of the Evidence Act." Paper prints of computer-generated electronic records stored on optical or magnetic media are acceptable as documents under Section 65B, subsection (1), provided that the requirements outlined in Subsection (2) of Section 65B are met. Section 65 of the Evidence Act may also be used to lead 'secondary evidence' regarding the document's contents.

APPRECIATION OF EVIDENCE RECORDED THROUGH ELECTRONIC MEDIA

i.Presumptions Applied to Electronic Data

Interpreting a relevant and admissible fact as having been proved is unnecessary. To determine if a fact is proven, the judge must find merit in the evidence. The existence of specific facts listed in the Evidence Act that the court may be

supposed to exist constitutes an exception to this general rule. Amendments have introduced various presumptions involving 'digital evidence' to the Evidence Act.(Karia, 2008)

ii.Electronic Gazettes
The authenticity of electronic records claiming to be from the Official Gazette or any other legally governed electronic record is presumed by the court under Section 8lA of the Evidence Act, so long as the record is produced from proper custody and is maintained predominantly in the form required by law.

iii. Electronic agreements
The Evidence Act's Section 84A establishes the presumption that a contract has been completed when digital signatures from both parties are attached to an electronic document that seems to be an agreement.

iv.Electronic messages
The 'electronic message' entered into the sender's computer for transmission is assumed to match the message forwarded by the sender to the addressee via an electronic mail server under the terms of Section 88A. That being said, no presumptions are made about the sender of the communication. This clause presumes that the electronic message is authentic; it makes no assumptions about the message's originator.

v. Electronic records dating back five years
According to Section 90A of the 'Evidence Act', it may be presumed that the digital signature appended to a document was applied by the signatory or a representative designated by the signatory if the record is produced from custody that the court deems appropriate and claims to be five years old. If an electronic record is in the appropriate place and handled by the person who would normally be responsible for it, then it is in proper custody. However, if it can be demonstrated that the record originated lawfully or if the case's specific facts make the origin likely, then custody is not deemed unlawful. Evidence submitted in the form of an electronic copy of the Official Gazette is likewise subject to the same requirement.

vi. Banker's Book Evidence Act Modifications
The printout of data from a floppy disk or any other electromagnetic device is now included in the definition of 'banker's book' (Section 2(3)). According to Section 2A, a printout of an entry or a copy of a printout must be accompanied by a certificate from the principal accountant or branch manager attesting to the printout's authenticity and by a certificate from the person in charge of the computer system that includes a brief description of the system and details about its security.

vii. Electronic evidence when relevant (Section 47A)
The view of the Certifying Authority that issued the 'Electronic Signature Certificate' is a relevant fact when the Court is asked to determine the electronic signature of any individual.

viii. Electronic agreement presumption (Section 85 A)
The Court will assume that any electronic document purportedly representing an agreement with the parties' electronic signatures was reached by attaching the parties' electronic signatures.

ix. Rules, regulations, etc., are published in the Electronic Gazette (Sec. 8)
Any 'rule', 'regulation', 'order', 'bye-law', 'notification', or other matter that is required by law to be published in the 'Official Gazette' will be considered to have satisfied this requirement if it is published in either the 'Official Gazette' or the 'Electronic Gazette'.

JUDICIAL PERSPECTIVE ON ELECTRONIC EVIDENCE
In 'State of Punjab v. Amritsar Beverages Ltd.'(2006), the Sales Tax Department searched the dealer's property and took documents and computer hard drives from it. The 'Punjab General Sales Tax Act of 1948', Section 14 stipulated that "authorities must return seized documents within a certain amount of time (Section 14(3)), as long as the dealer or other person in question receives a receipt for the property." Under these provisions, the computer hard disk was seized.
The speaker of the State of Haryana's Legislative Assembly 'disqualified a member for defecting' in the case of Jagjit Singh v. State of Haryana(2006). The Supreme Court considered the value of 'digital evidence' throughout its hearing, which included interview transcripts from the television networks 'Zee News,' 'Aaj Tak,' and 'Haryana News' of 'Punjab Today.'
Following the attack on Parliament on December 13, 2001, there was an appeal against the 'conviction' in 'State (NCT of Delhi)'(2005). A submission was made on behalf of the accused during the consideration of the appeal against them for attacking Parliament, arguing that "no reliance could be placed on the mobile call records because the prosecution had neglected to produce the necessary certificate under Section 65B(4) of the Evidence Act." This case concerned the admissibility and proof of 'mobile phone call records'. The SC concluded that the "call records could be proven by a

cross-examination of the competent witness who was acquainted with how the computer operated during the pertinent period and how the printouts of the call records were made."

The High Court of Calcutta ruled in 'Abdul Rahaman Kunji Vs. The State of West Bengal'(2014), that "an email that is downloaded and printed from an individual's email account can be used as proof under Section 65B r/w Section 88A of the Evidence Act. To demonstrate electronic communication, the witness's testimony that they followed the appropriate steps to download and print the material is acceptable."
A secondary piece of evidence, an 'electronic record', cannot be entered into evidence. The court noted that "an electronic record used as secondary evidence cannot be accepted into evidence unless section 65-B conditions are met."('Anvar P.V.'2014). "When it comes to 'CDs', 'VCDs', ''chips, and other similar devices, they must be accompanied by the section 65-B certificate that was received at the time of the evidence-taking. If this certificate is absent, the secondary evidence relevant to that electronic record is not admissible."

In the case of 'Sharad Yadav Vs. Union of India'(1999).,- a Hindi-language interview in which ' Sharad Yadav' acknowledged receiving Rs. 3 lacs from a Jain was broadcasted on Doordarshan following the appropriate editing. It was noted that the video recordings of Shri Sharad Yadav do not constitute confession and, as such, cannot be used to fulfill the crime for which he was charged.
In the case of 'Sajidbeg Asifbeg Mirza v. State of Gujarat'(2011) The Gujarat High Court held that "We believe that Afzal's conversation with the press and television, which he admittedly had while under police custody and in the immediate presence of the police, should not be relied upon," the court said, "regardless of whether the statement was made to a police officer as defined by Section 162 CrPC, we are not willing to give the statements made at the police-arranged interview any weight or reliability."

The Supreme Court noted in 'State of Maharashtra vs. Dr. Praful B Desai'(2003) that video conferencing is a scientific and technological advancement that allows one to see, hear, and converse with someone who is not physically present with the same ease and convenience as if they were. In this case, the court permitted the witness examination via video conference; it was observed that "There is no reason why the examination of a witness by video conference should not be an essential part of electronic evidence." It was decided in 'Amitabh Bagchi vs. Ena Bagchi'(2005) that "a person may be able to introduce evidence virtually, such as through video conferencing, and that a person's personal presence in court may not be necessary."

According to the distinction made by the court in 'Dharambir v. Central Bureau of Investigation'(2007), there are two tiers of an electronic record. The first is the 'hard disk', which, once in use, turns into an 'electronic record' of the data about the modifications it has undergone and the data that can be retrieved from it with software. The 'active and accessible data' stored on a hard drive in the format of a 'text file,' 'music file,' 'video file,' etc., is the other level of an 'electronic record.' Accessible data can be transformed or replicated to another magnetic or electronic device, such as a 'CD,' 'pen drive,' etc. A cloned disk or mirror image can be created from a blank hard drive devoid of any data yet previously utilized for data recording.

The SC in 'Anvar P.V'(2014) held that "computer output cannot be admitted without complying with 65b of Evidence Act and overrule the decision made by the two-judge Supreme Court bench in 'State (NCT of Delhi)'(2005). The court noted that "the ruling in, 'State (NCT of Delhi)' which deals with the admissibility of electronic evidence related to this court's electronic record, does not establish the proper position and must be overruled." The court's legal interpretation of the Evidence Act sections—22A, 45A, 59, 65A, and 65B—confirmed that "the stored data on CDs, DVDs, and pen drives is not admissible without a certificate under Section 65 B(4) of the Evidence Act. It also made clear that, in the absence of such a certificate, oral testimony cannot be used to establish the existence of such electronic evidence, nor can the expert opinion under Section 45A of the Evidence Act be used to demonstrate its authenticity."

ELECTRONIC EVIDENCE ADMISSIBILITY UNDER THE BHARATIYA SAKSHYA ADHINIYAM
A major step towards modernizing India's justice delivery system has been taken with the 'Bharatiya Sakshya Adhiniyam, 2023' (BSA) replacing the 'Indian Evidence Act, 1872' (IEA). This new law aims to make presenting and interpreting evidence in court more efficient, contemporary, and straightforward. The definition of 'evidence' under Section 2(e) of BSA includes 'statements given electronically,' and 'electronic and digital records' in the definition of 'document,' which includes a wide variety of 'electronic records.' 'Emails', 'server logs', 'files saved on PCs', 'laptops', or 'smartphones', 'text messages', 'website content', 'location data', 'voice mails,' and 'messages' saved on 'digital devices' are just a few examples of the wide range of 'electronic records' that are now included in this term(Section 2,d). Important changes made in BSA in terms of the admissibility of digital or electronic evidence are as follows:

Section 61 of the BSA stipulates that "Nothing in this Adhiniyam shall apply to deny the admissibility of an electronic or digital record in the evidence on the ground that it is an electronic or digital record and such record shall, subject to section 63, have the same legal effect, validity, and enforceability as other documents." This Section accords electronic recordings the same weight as documentary evidence, as previously established by the 'Information Technology Act of 2000' and the 'Indian Evidence Act of 1872'. In addition to the three justifications listed in the IEA, the BSA under Section 57 defines 'primary evidence' and includes four additional justifications, numbered 4, 5, 6, and 7. The following four situations would qualify as primary evidence under the BSA requirements for electronic or digital records: -

A. According to Explanation 4, "Where an electronic or digital record is created or stored, and such storage occurs simultaneously or sequentially in multiple files, each such file is primary evidence."
B. According to explanation 5, "Where an electronic or digital record is produced from proper custody, such electronic and digital record is primary evidence unless it is disputed."
C. Explanation 6 states, "Where a video recording is simultaneously stored in electronic form and transmitted or broadcast or transferred to another, each of the stored recordings is primary evidence."
D. Explanation 7 states, "Where an electronic or digital record is stored in multiple storage spaces in a computer resource, each such automated storage, including temporary files, is primary evidence."

The definition of 'document' and 'evidence' has been expanded by BSA to include any matter expressed, described, or otherwise recorded upon any substance through 'letters,' 'figures,' 'marks', or any other means or by more than one of those means, intended to be used, or which may be used, to record that matter. This definition also includes 'electronic and digital records', which were not included in the IEA's definition of 'document.' Furthermore, to account for 'electronic records', a new illustration (vi) was included in the definition of 'documents' – "An electronic record on emails, server logs, documents on computers, laptop, or smartphone, messages, websites, locational evidence and voice mail messages stored on digital devices are documents." (section 2 d)

Comparably, the BSA expanded the scope of evidence to include,'information given electronically' in oral testimony and 'or digital records' in documentary testimony, which was not there in the IEA. Broadening the definition of 'electronic evidence': The BSA substantially improves the 'electronic evidence' field, incorporating primary and secondary evidence considerations and important revisions. In addition to 'records on paper' and 'records stored,' recorded, or duplicated on 'optical' or 'magnetic media, section 63 of the BSA now includes 'electronic records stored in semiconductor memories.' Moreover, the clause expands the scope of its use to include 'any communication device.' The definition of a 'computer' or 'communication device' is improved and given a more thorough meaning in subsection (3) of the provision.
It's crucial to remember that BSA Section 63's sub-section (4) upholds the IEA's Section 65B (4)'s requirement for a 'certificate', but it adds that the ''certificate needs to be submitted with the 'electronic record' each time 'electronic evidence' is used in court. Furthermore, the amended clause clarifies that anybody "in charge of the computer or communication device and an expert (whichever is appropriate)" can issue the certificate, removing the previous need that the individual has a 'responsible official position.'

CONCLUSION

The exploration of 'electronic evidence' within the framework of Indian jurisprudence highlights the evolving nature of legal standards concerning the admissibility and reliability of such evidence. Through various landmark cases, including 'Sharad Yadav(1999) and Sajidbeg Asifbeg(2011), courts are increasingly cautious regarding the circumstances under which 'electronic evidence' is collected and presented. The need for fairness and the preservation of the rights of the accused remain paramount in judicial considerations, as highlighted by the observations made by Dr. Praful B. Desai(2003) and other significant rulings.

The introduction of the 'Bharatiya Sakshya Adhiniyam, 2023' marks a crucial step toward modernizing the legal framework governing 'electronic evidence'. By treating 'digital records' on par with traditional documents and expanding definitions to encompass various forms of electronic communication, this new legislation acknowledges the significance of technology in the contemporary legal landscape. However, the reliance on certificates for the admissibility of electronic evidence, as mandated by both the 'Indian Evidence Act[1]' and the 'Bharatiya Sakshya Adhiniyam'[2], underscores the necessity of strict adherence to procedural requirements to prevent misuse and ensure the integrity of the judicial process.

To adhere to this, the author suggests the following things that can help fulfill the legislature's purpose. Firstly, As technology advances, clearer guidelines should be established regarding the admissibility of evidence gathered through video conferencing, especially ensuring that the rights of the accused are protected. Secondly, The requirement for certificates accompanying electronic evidence should be standardized, ensuring that they are easily understandable and

[1] Indian Evidence Act, No. 1, Acts of Parliament, 1872 (India).

[2] Bharatiya Sakshya Adhiniyam, No. 12, Acts of Parliament, 2023 (India).

accessible. This would facilitate smoother judicial processes and reduce confusion regarding compliance. Thirdly, Law enforcement agencies should receive training on the proper methods for collecting, storing, and presenting 'electronic evidence' to ensure that it adheres to legal standards and maintains its integrity. Fourthly, Initiatives to raise public awareness about the rights of individuals concerning 'electronic evidence' collection and the implications of such evidence in legal proceedings should be implemented. Fifthly, it is imperative that lawmakers continuously assess and amend existing legal frameworks to address emerging challenges in the realm of 'electronic evidence', ensuring that justice is both timely and equitable. By addressing these suggestions, the legal framework surrounding 'electronic evidence' in India can be strengthened, fostering a judicial environment that effectively balances technological advancements with the principles of justice and fairness.

REFERENCES

1. Abdul Rahaman Kunji v. State of West Bengal, (2014) 2 CHN 754 (Cal).
2. Amitabh Bagchi v. Ena Bagchi, AIR 2005 Cal 11 (AIR 2005 Cal 11).
3. Anvar P.V. v. P.K. Basheer & Ors., (2014) 10 SCC 473.
4. Anvar P.V. v. P.K. Basheer & Others, (2014) 10 SCC 473.
5. Banker's Book Evidence Act, No. 18, Acts of Parliament, 1891 (India).
6. Banker's Book Evidence Act, No. 18, Acts of Parliament, 1891 (India).
7. Bharatiya Sakshya Adhiniyam, No. 12, Acts of Parliament, 2023 (India).
8. Black's Law Dictionary (10th ed. 2014).
9. Dharambir v. Central Bureau of Investigation, (2007) 139 DLT 289 (Del).
10. Indian Evidence Act, No. 1, Acts of Parliament, 1872 (India).
11. Indian Penal Code, No. 45, Acts of Parliament, 1860 (India).
12. Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
13. Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
14. Jagjit Singh v. State of Haryana, (2006) 11 SCC 1.
15. Punjab General Sales Tax Act, 1948, No. 46, Acts of the Punjab State Legislature, 1948 (India).
16. Karia T. D. (2008) 'Digital Evidence: An Indian Perspective', Digital Evidence and Electronic Signature Law Review, Vol 5, available at https://core.ac.uk/download/pdf/20116845.pdf (accessed on July 20, 2024).
17. Sajidbeg Asifbeg Mirza v. State of Gujarat, (2011) 2 GLR 1741 (Guj).
18. Sharad Yadav & Ors. v. Union of India, (2003) 4 SCC 2.
19. State (NCT of Delhi) v. Navjot Sandhu alias Afzal Guru, (2005) 11 SCC 600.
20. State of Bihar v. Sri Radha Krishna (1983) 2 SCR 808.
21. State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601.
22. State of Punjab & Ors. v. M/S. Amritsar Beverages Ltd., AIR 2006 SC 2820.
23. Tomaso Bruno & Anr. v. State of U.P., (2015) 7 SCC 178.
24. United Nations Comm'n on Int'l Trade Law, Model Law on Electronic Commerce (1996).